National Infrastructure Protection Center
CyberNotes

Issue #2001-07 *April 9, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between March 5 and April 4, 2001. The table provides the vendor/operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Akopia[1]	Multiple	Interchange 4.5.3, 4.6.3	A vulnerability exists in the default installation of the sample files 'barry,' 'basic,' and 'construct,' which could let a malicious user read or change the customer data, product items, and order information.	No workaround or patch available at time of publishing.	Akopia Interchange Sample Files	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Alt-N[2]	Windows 95/98/NT 4.0/2000	MDaemon 3.5.6	A Denial of Service vulnerability exists when a large 'SELECT' or 'EXAMINE' command is sent.	No workaround or patch available at time of publishing.	MDaemon IMAP Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Securiteam, March 25, 2001.
[2] Bugtraq, March 25, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Anaconda[3]	Multiple	Clipper 3.3	A directory traversal vulnerability exists which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Clipper Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Apache Group[4]	Unix	Tomcat 3.0	A directory traversal vulnerability exists which could let a remote malicious user gain sensitive information.	Upgrade available at: http://jakarta.apache.org/builds/jakarta-tomcat/release/v3.2.2-beta-2/bin/	Tomcat Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Apache Group[5]	Windows 98/ME/NT 4.0/2000, Unix	Apache 1.3.12 , 1.3.17, 1.3.17win32, 1.3.3, 1.3.9	A vulnerability exists when a custom crafted request is sent to the server, which could let a remote malicious user obtain a listing of the directory contents. This could potentially result in a compromise of the system.	Upgrade available at: http://httpd.apache.org/dist/apache_1.3.19.tar.gz	Apache Artificially Long Slash Path Directory Listing	**High**	Bug discussed in newsgroups and websites.
Argus Systems[6]	Unix	PitBull LX All versions	A vulnerability exists in the syscatl() system function, which could allow a malicious user to read system configuration information, bypass the security restrictions, and tamper with the system.	Patch available at: http://archives.neohapsis.com/archives/bugtraq/2001-03/0485.html	Pitbull LX sysctl()	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Axent Technol-ogies, Inc.[7]	Windows NT 4.0, Unix	Raptor 6.5	A vulnerability exists which could allow a malicious user to access private web resources and gain sensitive information if the http forwarding module has been enabled (which is the default setting).	Patch available at: ftp://ftp.axent.com/pub/RaptorFirewall/Patches/6.50/Internal/http-int.zip	Raptor Firewall HTTP Request Proxying	Medium/ **High** **(High if DDoS best practices not in place.)**	Bug discussed in newsgroups and websites. Exploit has been published.
BEA Systems[8]	Windows 95/98/NT 4.0/2000, Unix	WebLogic Server 4.5.1, 5.1, 6.0	A directory traversal vulnerability exists which could let a malicious user gain sensitive information.	Patch available at: http://commerce.bea.com/downloads/weblogic_server.jsp#wls	WebLogic Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Caucho Technology[9]	Windows 2000, Unix	Resin 1.2, 1.3	A specially constructed HTTP request could enable a remote malicious user to gain read access to any known JavaBean file.	No workaround or patch available at time of publishing.	Resin JavaBean Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[3] UkR Security Team, Advisory No. 11, March 27, 2001.
[4] CHINANSL Security Advisory, CSA-200105, March 31, 2001.
[5] eSecurityOnline Free Vulnerability Alert 3462, March 14, 2001.
[6] Securiteam, March 31, 2001.
[7] Bugtraq, March 24, 2001.
[8] Defcom Labs Advisory, def-2001-14 re-release, March 27, 2001.
[9] CHINANSL Security Advisory, CSA-200111, April 4, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[10]	Multiple	Cisco Content Services Switch (CSS 11050, CSS 11150, and CSS 11800) (also known as Arrow point)	A vulnerability exists which could allow non-privileged malicious users to escalate their privilege level and gain administrative access.	Upgrade available at: http://www.cisco.com/cgi-bin/tablebuild.pl/webns	Cisco Content Services User Account	**High**	Bug discussed in newsgroups and websites.
Cisco Systems[11]	Multiple	VPN 3000 concen-trators running software releases up to 3.0.00	A remote Denial of Service vulnerability exists because the SSL or regular Telnet session does not disconnect after repeated failed attempts.	Upgrade available at: regular update channels. www.cisco.com	Cisco VPN3000 Concentrator Telnet Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Computer Associates [12]	Windows NT 4.0/2000	CCC\ Harvest 5.0	A vulnerability exists in the control software password encryption, which could let a malicious user gain superuser status.	No workaround or patch available at time of publishing.	CCC\Harvest Source Code Control Software Password Encryption	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Conectiva[13]	Unix	Linux 4.0, 4.0es, 4.1, 4.2, 5.0, prg graficos, ecommerce, 5.1, 6.0	Several buffer overflow vulnerabilities exist which could let a remote malicious user cause a Denial of Service.	Upgrade available at: ftp://atualizacoes.conectiva.com.br/	IMAP Multiple Remote Buffer Overflows	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Conectiva[14]	Unix	Zope-2.1.x	Multiple vulnerabilities exist; a local role computation vulnerability which could let a malicious user elevate privileges; a vulnerability in DTML which could let a malicious user with DTML editing privileges edit the data of a file or image object via DTML; and a vulnerability in the POST command.	Upgrade available at: ftp://atualizacoes.conectiva.com.br/	Zope Multiple Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Conectiva Linux[15] and SUSE[16]	Unix	Conectiva Linux 6.0; SuSE 7.1	Several local and remote buffer overflow and insecure temporary file handling vulnerabilities exist, which could let a local or remote malicious user gain root access.	Upgrade available at: **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br/6.0/ **SuSE:** ftp://ftp.suse.com/pub/suse/i386/update/7.1/	Multiple Cups Vulnerabilities	**High**	Bug discussed in newsgroups and websites.

[10] Cisco Security Advisory, April 4, 2001.
[11] Cisco Security Advisory, March 28, 2001.
[12] Zero Tolerance Technologies (T) Security Advisory, ZTT-SA01-27032001, March 28, 2001.
[13] Conectiva Linux Security Announcement, CLA-2001:388, March 19, 2001.
[14] Conectiva Linux Security Announcement, CLA-2000:365, March 20, 2001.
[15] Conectiva Linux Security Announcement, CLA-2001:386, March 16, 2001.
[16] SuSE Security Announcement, SuSE-SA:2001:05, March 5, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Data General[17]	Unix	DG/UX 4.20MU02, 4.20MU06	A vulnerability exists in the way error messages are handled by the printer scheduler, which could allow a malicious user to execute arbitrary code.	No workaround or patch available at time of publishing.	DG/UX lpsched Long Error Message Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Elron Software, Inc.[18]	Multiple	IM Message Inspector 3.0.3; IM Anti-Virus 3.0.3	A directory traversal vulnerability exists which could let a malicious user gain confidential data.	Update available at: http://www.elronsw.com/	IM Message Inspector and IM AntiVirus Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Francisco Burzi[19]	Multiple	PHP-Nuke 4.4.1a	A vulnerability exists in the XML parser, which could allow a malicious user to execute arbitrary commands.	No workaround or patch available at time of publishing.	PHP-Nuke XML Parser	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
FTPFS[20]	Unix	FTPFS 0.1.1k2.2, 0.1.1k2.4, 0.2.1k2.4, 0.2.2k2.4	A buffer overflow vulnerability exists due to insufficient bounds checking, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.	No workaround or patch available at time of publishing.	FTPFS mount Buffer Overflow	Low/**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Gene6[21]	Windows 95/98/ME/ NT 4.0/2000	G6 FTP Server 2.0 (now known as BFTP)	A vulnerability exists in the 'size' and 'mdtm' ftp commands if the 'show relative paths' option is not set, which could allow a malicious user to map the directory structure of the system by requesting attributes of known system files.	Upgrade available at: http://www.bpftpserver.com/download.html	G6 FTP File Existence Disclosure and NetBIOS Hash Retrieval CVE Name: CAN-2001-0263, CAN-2001-0264	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Hursley Software Labora-tories[22]	Unix	Hursley Software Laboratories Consumer Transaction Framework (HSLCTF) 1.0 for AIX	A Denial of Service vulnerability exists in the HTTP object.	Contact vendor for workaround.	Hursley Software Laboratories Consumer Transaction Framework Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
IBM[23]	Unix	WCS (WebSphere Commerce Suite) 4.0.1 with Application Server 3.0.2	A vulnerability exists which could let a malicious user download the original source code of JSP files.	Upgrade available at: http://www.ibm.com/software/webservers/appserv/efi	WCS JSP Source Code Exposure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[17] Bugtraq, March 19, 2001.
[18] Bugtraq, March 23, 2001.
[19] Securiteam, March 26, 2001.
[20] Securiteam, March 14, 2001.
[21] @stake, Inc Security Advisory, A040301-1, April 3, 2001.
[22] Defcom Labs Advisory, def-2001-12, March 20, 2001.
[23] CHINANSL Security Advisory, CSA-200107, March 29, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Infradig[24]	Windows 95/98/NT 4.0/2000, Unix	Inframail 3.80a-3.97a	A remote Denial of Service vulnerability exists due to a malformed POST request.	Upgrade available at: http://www.infradig.com/ftp/inframail.exe	Inframail Post Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Michael A. Gumienny [25]	Unix	FCheck 2.6.27, 2.7.34, 2.7.38, 2.7.40, 2.7.45-2.7.47, 2.7.50-2.7.51, 2.7.58	A vulnerability exists due to an insecurely structured call to open(), which could let a malicious user execute arbitrary commands.	FCheck v2.07.58 and earlier [are] no longer supported.	FCheck Local Command Execution	**High**	Bug discussed in newsgroups and websites.
Microsoft[26]	Windows 98/ME	Microsoft Plus! 98, Windows ME	A vulnerability exists in the implementation of the password protection option, which could let a malicious user recover data compression passwords.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-019.asp.	Plus! 98 and Windows ME Recoverable Compressed Folder Passwords CVE Name: CAN-2001-0152	Medium	Bug discussed in newsgroups and websites.
Microsoft[27]	Windows 2000	Internet Security and Acceleration Server 2000	A Denial of Service vulnerability exists if an alert action has been chosen in the ISA server console.	For information on properly configuring the server, please see the article at: www.microsoft.com/technet/support/kb.asp?ID=284800	Internet & Acceleration Server Event Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[28]	Windows 2000	Internet Explorer 5.x, Internet Information Service 5.0. Exchange 2000	A vulnerability exists due to the interaction between IE 5.x, IIS 5.0, and Exchange 2000. If a malicious web page is browsed with IE, it is possible to list the directories of arbitrary IIS 5.0 servers. Under certain circumstances, it is also possible to read the user's e-mail or folders if they are stored on an Exchange 2000 server, and possibly create or modify files.	Temporary workaround (Georgi Guninski): Disable Active Scripting.	IE, IIS and Exchange 2000 Interaction	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the Press and other public media.
Microsoft[29]	Windows	Internet Explorer 5.5	A vulnerability exists in the ActiveX object 'MSScriptControl.Script Control' in combination with GetObject that could let a malicious user read arbitrary local files and send them to an arbitrary server.	Unofficial workaround (Georgi Guninski): Disable Active Scripting.	Internet Explorer 'MSScript Control.Script Control'	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[24] Strumpf Noir Society Advisories, March 28, 2001.
[25] Securiteam, March 24, 2001.
[26] Microsoft Security Bulletin, MS01-019, March 29, 2001.
[27] Defcom Labs Advisory, def-2001-16, April 2, 2001.
[28] Georgi Guninski Security Advisory #40, March 28, 2001.
[29] Georgi Guninski Security Advisory #41, March 31, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[30]	Windows 2000/NT 4.0	Windows 2000, NT 4.0	A vulnerability exists due to a flaw in the implementation of Dr. Watson, which could let a malicious user obtain sensitive information such as users' mail passwords or other private data.	No workaround or patch available at time of publishing.	Windows NT Dr. Watson 'user.dmp' Permissions	Medium	Bug discussed in newsgroups and websites.
Microsoft[31] ***Microsoft Security Bulletin Update***[32]	**Windows 95, 98, ME, NT 4.0, 2000**	**Windows 95, 98, ME, NT 4.0, 2000**	**VeriSign, Inc., recently advised Microsoft that on January 29 and 30, 2001, it issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee. The common name assigned to both certificates is "Microsoft Corporation."** ***The software update discussed in the original version of the bulletin is now available.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/MS01-017.asp**	**Unauthenti - cated "Microsoft Corporation" Certificates**	**Medium**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the Press and other public media.**
Microsoft[33]	Windows 95/98/NT 4.0/2000	Internet Explorer 5.01, 5.5	A vulnerability exists in the type of processing that is specified for certain unusual MIME types. This could let a malicious user modify the MIME header information to specify that the attachment was one of the unusual MIME types that IE handles. This could also lead to the execution of arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-020.asp	Internet Explorer Incorrect MIME Header CVE Name: CAN-2001-0154	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[34]	Windows NT 4.0	Visual Studio 6.0 Enterprise Edition, Visual Basic 6.0 Enterprise Edition	An unchecked buffer vulnerability exists in the VB-TSQL debugger object, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-018.asp	Visual Studio VB-TSQL Object Unchecked Buffer CVE Name: CAN-2001-0153	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[35]	Unix	MIT Kerberos 5, (all releases prior to krb5-1.2.2-beta1), MIT Kerberos 4 patch 10, and earlier	Multiple vulnerabilities exist which could let a malicious user overwrite files and achieve root access.	Contact your vendor for upgrade.	MIT Kerberos Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[30] Securiteam, March 27, 2001.
[31] Microsoft Security Bulletin, MS01-017, March 22, 2001.
[32] Microsoft Security Bulletin, MS01-017 (version 2.0), March 28, 2001.
[33] Microsoft Security Bulletin, MS01-020, March 29, 2001.
[34] Microsoft Security Bulletin, MS01-018, March 27, 2001.
[35] eSecurityOnline Free Vulnerability Alert 3451, March 9, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[36]	Unix	Dave Mills Xntp3 5.93-5.93e, Xntp 4.0.99-4.0.99k	A buffer overflow vulnerability exists which could let a remote malicious crash the daemon or execute arbitrary code on the host.	**Mandrake-Linux:** http://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates/ **FreeBSD:** http://phk.freebsd.dk/patch/ntpd.patch **Debian:** http://security.debian.org/debian-security/dists/stable/updates/main/	Ntpd Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[37]	Windows 95/98/NT 4.0/2000, Unix	Apache Group Tomcat 4.0; BEA Systems Weblogic Server 5.1	A vulnerability exists when an HTTP request is appended with certain characters, which will reveal the source code of JSP files. Such source code may contain database passwords and file names.	Upgrade to 4.0 beta 3 available at: http://jakarta.apache.org/builds/jakarta-tomcat-4.0/release/v4.0-b3/	Multiple Vendor URL JSP Request Source Code Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple Vendors[38, 39]	Unix	Conectiva Linux 4.1, 4.2, 5.0, 5.1, 6.0; Icecast versions prior to 1.3.7_1	Several buffer overflow and format string vulnerabilities exist, which could let a remote malicious user execute arbitrary code.	Upgrade available at: **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/	Icecast Remote Buffer Overflow and Format String	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[40, 41, 42, 43]	Unix	Red Hat Linux 5.2 alpha, i386, sparc, 6.2 alpha, i386, sparc, 7.0 alpha, i386; Immunix OS 6.2, 7.0-beta, and 7.0; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, prg graficos, ecommerce, 5.1; Trustix Secure Linux 1.2	A format string vulnerability exists in the IMAP code, which could let a malicious user execute arbitrary code.	Updates available at: **RedHat:** ftp://updates.redhat.com/ **Immunix:** http://immunix.org/ImmunixOS/6.2/updates/ **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br **Trustix:** http://www.trusix.net/pub/Trustix/updates/	Mutt Format String	**High**	Bug discussed in newsgroups and websites.

[36] Bugtraq, April 4, 2001.
[37] CHINANSL Security Advisory, CSA-200110, April 1, 2001.
[38] Conectiva Linux Security Announcement, CLA-2001:387, March 19, 2001.
[39] FreeBSD Ports Security Advisory, FreeBSD-SA-01:23, March 12, 2001.
[40] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:029-02, March 13, 2001.
[41] Immunix OS Security Advisory, IMNX-2001-70-006-01, March 15, 2001.
[42] Conectiva Linux Security Announcement, CLA-2001:385, March 16, 2001.
[43] Trustix Secure Linux Security Advisory #2001-0001, March 16, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[44, 45, 46, 47, 48]	Unix	SLRN Development Team slrn 0.9.6.2-9, 0.9.6.3, 0.9.6.4	A buffer overflow vulnerability exists when the wrapping/ unwrapping function is enabled, which could let a malicious user execute arbitrary code.	Updates available at: **RedHat:** ftp://updates.redhat.com/ **Immunix:** http://immunix.org/ImmunixOS/6.2/updates/ **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3 **Debian**: http://security.debian.org/dists/stable/updates/ **Conectiva:** ftp://atualizacoes.conectiva.com.br	SLRN Long Header Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Multiple Vendors[49, 50, 51, 52, 53]	Unix	Cees De Groot SGMLtools 1.0.7, 1.0.9	A vulnerability exists due to insecure handling of temporary file permissions, which could let a malicious user overwrite and corrupt the documents of other users.	Update available at: **RedHat:** ftp://updates.redhat.com/ **Immunix:** http://immunix.org/ImmunixOS/6.2/updates/RPMS **Linux-Mandrake:** http://www.linux-mandrake.com/en/ftp.php3 **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/dists/stable/updates/main	SGMLtools Temporary File Permission	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[44] Debian Security Advisory, DSA-040-1, March 9, 2001.
[45] Linux-Mandrake Security Update Advisory, MDKSA-2001:028, March 9, 2001.
[46] Immunix OS Security Advisory, IMNX-2001-70-007-01, March 15, 2001.
[47] Conectiva Linux Security Announcement, CLA-2001:383, March 14, 2001.
[48] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:028-02, March 13, 2001.
[49] Red Hat, Inc. Red Hat Security Advisory , RHSA-2001:027-02, March 14, 2001.
[50] Immunix OS Security Advisory, IMNX-2001-70-008-01, March 15, 2001.
[51] Linux-Mandrake Security Update Advisory, MDKSA-2001:030-1, March 20, 2001.
[52] Conectiva Linux Security Announcement, CLA-2001:390, March 27, 2001.
[53] Debian Security Advisory, DSA-038-1, March 8, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[54, 55, 56, 57, 58]	Unix	Linux Mandrake 7.0, 7.1, 7.2, Corporate Server 1.0.1; Immunix OS 6.2, 7.0-beta, 7.0; Red Hat Linux 7.0; Conectiva Linux 5.0, prg graficos, ecommerce, 5.1, 6.0; Trustix Secure Linux 1.01, 1.1, 1.2; OpenSSH 2.5.2	Multiple vulnerabilities exist in various implementations of SSH protocols which could let a malicious user obtain sensitive information by passively monitoring encrypted SSH sessions.	**LinuxMandrake:** http://www.linux-mandrake.com/en/ftp.php3 **Immunix:** http://immunix.org/ImmunixOS/6.2/updates/RPMS **RedHat:** ftp://updates.redhat.com/7.0/ **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br/ **Trustix:** ftp.trusix.net/pub/Trustix/updates/ **OpenSSH:** http://www.openssh.com/	Multiple OpenSSH Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Multiple[59, 60]	Unix	FreeBSD 3.5, 4.2; Mandrake Soft Corporate Server 1.0.1, Linux Mandrake 6.0-7.2	A Denial of Service vulnerability exists when a malicious user sends malformed packets consisting of less information than expected.	Patches available at: **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-01:28/timed.patch **MandrakeSoft Corporate Server 1.0.1:** ftp://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates/1.0.1/RPMS/timed-0.17-1.2mdk.i586.rpm **MandrakeSoft Linux:** ftp://sunsite.ualberta.ca/pub/Mirror/Linux/mandrake/updates/	Timed Small Packet Denial of Service	Low	Bug discussed in newsgroups and websites.

[54] Linux-Mandrake Security Update Advisory, MDKSA-2001: 033-1, March 23, 2001.
[55] Immunix OS Security Advisory, IMNX-2001-70-009-01, March 26, 2001.
[56] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:041-02, April 4, 2001.
[57] Conectiva Linux Security Announcement, CLA-2001:391, March 28, 2001.
[58] Trustix Secure Linux Security Advisory, #2001-0002, March 29, 2001.
[59] FreeBSD Security Advisory, FreeBSD-SA-01:28, March 12, 2001.
[60] Linux-Mandrake Security Update Advisory, MDKSA-2001:034, March 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple[61, 62, 63]	Unix	Linux Mandrake 7.1, 7.2, Corporate Server 1.0.1; RedHat Linux 7.0, Powertools; Conectiva Linux 4.0, 4.0es, 4.1, 4.2, 5.0, prg graficos, ecommerce, 5.1, 6.0	Two vulnerabilities exist: a buffer overflow in the logging code; and an unguarded system() call when receiving an URL which could let a remote malicious user execute arbitrary commands.	**LinuxMandrake:** http://www.linux-mandrake.com/en/ftp.php3 **RedHat:** ftp://updates.redhat.com/ **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br	Multiple Vendor LICQ Buffer Overflow And URL Command Execution	High	Bug discussed in newsgroups and websites.
Navision[64]	Windows NT 4.0/2000, Unix	Navision Financials Server 2.50, 2.60	A remote Denial of Service vulnerability exists when invalid input is submitted to a server listening on port 2407.	Patch available at: http://www.navision.com/com/view.asp?documentID=258	Navision Financials Server Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
NetScreen [65]	Multiple	ScreenOS 1.64, 1.66, 2.1, 2.5	A vulnerability exists that could potentially allow malicious packets to pass to the DMZ network, which could impact systems on the network.	If you have registered your product with NetScreen and have a service contract, an upgrade is available at: http://www.netscreen.com/support/updates.html	NetScreen ScreenOS Firewall Policy Bypass	Medium	Bug discussed in newsgroups and websites.
OReilly Software[66]	Windows 95/98/NT 4.0/2000	Website Pro 3.0.37	A remote Denial of Service vulnerability exists due to a memory leak if non-authenticated requests are repeatedly made to the /dyn/ directory.	Unofficial workaround (Defcon Labs): Disallow access to the remote manager service from untrusted networks. The service is on TCP port 9999 by default.	Website Pro Remote Manager Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Quest Software[67]	Unix	SharePlex 2.1.3.9, 2.2.2 beta	A vulnerability exists in the Qview component, which could let a malicious user read any file on the system and elevate their privileges.	Upgrade available at: www.quest.com/shareplex	SharePlex Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Raytheon[68]	Multiple	Silent Runner Collector 1.6.1	A buffer overflow vulnerability exists when a long HELO command is issued, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Silent Runner HELO Buffer Overflow Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[61] Linux-Mandrake Security Update Advisory, MDKSA-2001:032, March 23, 2001.
[62] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:022-03, March 28, 2001.
[63] Conectiva Linux Security Announcement, CLA-2001:389, March 27, 2001.
[64] Defcom Labs Advisory, def-2001-17, April 3, 2001.
[65] SecurityFocus, March 26, 2001.
[66] Defcom Labs Advisory, def-2001-15, March 28, 2001.
[67] Securiteam, March 31, 2001.
[68] Securiteam, March 31, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Rit Research Labs[69]	Windows 95/98/NT 4.0	The Bat! 1.51	A security vulnerability exists which could allow a remote malicious user bypass some of the security features and save an attachment to places other than the temp directory. This could cause the user to execute malicious programs without warning.	This has been fixed in a beta version of the program which is available at: www.ritlabs.com/ftp/pub/the_bat/beta/tb152b03.rar	"The Bat!" Concealed Attachment	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SCO[70]	Unix	OpenServer 5.0.6	Buffer overflow vulnerabilities exist in the lpshut application, recon application, lpforms application, lpadmin application, deliver application, and the sendmail application which could allow a malicious user to elevate their privileges.	No workaround or patch available at time of publishing.	Multiple SCO Buffer Overflow Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Software 602[71]	Windows 95/98/NT 4.0/2000	602Pro LAN SUITE 2000a 2000.0.1.34	Two vulnerabilities exist: a buffer overflow vulnerability in WEBPROX.DLL; and a Denial of Service in the MS-DOS device file.	No workaround or patch available at time of publishing.	Lan Suite DOS Device Buffer Overflow and Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems, Inc.[72]	Unix	Solaris 2.5, 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86	A buffer overflow vulnerability exists due to improper handling of environment variables by tip, which could let a malicious user execute arbitrary code and gain root access.	Unofficial workaround (Bugtraq): Remove the suid uucp bit from the tip program.	Solaris tip Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Sun Microsystems, Inc.[73]	Unix	Solaris 2.X	A vulnerability exists in perfmon, which could allow a malicious user to create arbitrary files with root privileges.	Remove the setuid permission; contact your vendor for a patch.	Solaris Perfmon Root Privilege	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems, Inc. [74]	Windows 2000	JavaServer Web Development Kit (JSWDK) 1.0.1	A directory traversal vulnerability exists which could let a remote malicious user access files outside the root directory.	Update JSWDK	JavaServer Web Development Kit Directory Traversal	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
SurfControl [75]	Windows NT 4.0	SuperScout 3.0.1, 3.0.2	A vulnerability exists which could let a malicious user bypass 'Content Filtering" rules.	No workaround or patch available at time of publishing.	SuperScout for MS Proxy Site Filtering	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[69] Securiteam, April 3, 2001.
[70] Reconnaissance Team Security Advisories, SRT2001-02 through SRT2001-07, March 27, 2001.
[71] Securiteam, March 28, 2001.
[72] Bugtraq, March 27, 2001.
[73] Securiteam, March 24, 2001.
[74] CHINANSL Security Advisory, CSA-200106, March 29, 2001.
[75] Securiteam, March 23, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
T.C.X Data Konsult[76]	Unix	MySQL 3.20.32a, 3.23.34	A symbolic link vulnerability exists which could let a malicious user overwrite arbitrary files and lead to a root compromise.	Update available at: http://www.mysql.com/downloads/mysql-3.23.html	MySQL Root Operation Symbolic Link File Overwriting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Trend Micro Inc.[77]	Windows NT	ScanMail 3.5 for Exchange	A vulnerability exists due to a weak encoding scheme to store the administrative credentials, which could allow a malicious user gain the encoded credentials, decode them and use them to log on with administrative privileges.	Trend Micro recommends, as a temporary fix, that the following keys (and all sub-keys) should have their permissions set to Full Control for Administrators and SYSTEM (remove all other permissions): HKLM \Software\Trend Micro\ScanMail for Exchange\Remote Management and HKLM \Software\Trend Micro\ScanMail for Exchange \UserInfo	ScanMail Weak Encoding Scheme	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Trend Micro Inc.[78]	Windows 2000	Virus Buster 2001 (Japanese) 8.02	A buffer overflow vulnerability exists when MUA receives e-mail with a header containing long strings, which could let a malicious user execute arbitrary code.	Update available at: http://www.trendmicro.co.jp/homeuser/download/vb2001sp3.htm	Virus Buster 2001 Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
VIM Development Group[79, 80]	Unix	VIM 5.7	A vulnerability exists in the function system() command, which could let a malicious user embed arbitrary commands in a normal text file.	**RedHat:** ftp://updates.redhat.com/ **Mandrake-Linux:** http://www.linux-mandrake.com/en/ftp.php3	VIM statusline Text-Embedded Command Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[76] Securiteam, March 23, 2001.
[77] STAT Security Advisory, April 2, 2001.
[78] Bugtraq, March 30, 2001.
[79] Red Hat, Inc. Red Hat Security Advisory, RHSA-2001:008-02, March 21, 2001.
[80] Linux-Mandrake Security Update Advisory, MDKSA-2001:035, March 27, 2001.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system and/or the intruder can execute or alter arbitrary system files. An example of this would be a vulnerability, in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between March 19 and April 7, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 18 scripts, programs, and net-news messages containing holes or exploits were identified.
NOTE: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Script Description
April 7, 2001	Arpmim-0.2.tar.gz	Arpmim v0.2 implements an ARP man-in-the-middle attack and includes single or multiple host support.
April 6, 2001	Malevolence.sit	An exploit that allows users to view a unshadowed version of the /etc/password file on a Mac OS X computer.
April 6, 2001	Maxty.tar.gz	A small kernel-space TTY sniffer that will attach to read/write syscalls and save incoming/outgoing requests to opened TTY devices into separate log files.
April 6, 2001	Rnmap_0.5.2-beta.tar.gz	A python client/server package which allows many authorized clients to connect to a centralized nmap server to do their port scanning.
April 6, 2001	Scanssh-1.55.tar.gz	A scanner which scans a list of addresses and networks that are running SSH servers and their numbers.
April 6, 2001	Trafdisp.tgz	A sniffer which allows you to monitor the amount of incoming/outgoing KBps on a selected network interface(s) from at least one machine.
April 4, 2001	Ntpd-exp.c	Script which exploits the Ntpd Remote Buffer Overflow vulnerability.
April 3, 2001	G6-2nbt.pl	Perl script which exploits the G6 FTP File Existence Disclosure and NetBIOS Hash Retrieval vulnerability.
April 3, 2001	G6-find.pl.	Perl script which exploits the G6 FTP File Existence Disclosure and NetBIOS Hash Retrieval vulnerability.
March 29, 2001	**Iemsdaipp.txt**	**Example exploit for the IE, IIS and Exchange 2000 Interaction vulnerability.**
March 28, 2001	**Msdaippdemo.html**	**Exploit for the IE, IIS and Exchange 2000 Interaction vulnerability.**
March 27, 2001	Sara-3.3.5.tar.gz	A security analysis tool based on the SATAN model.

Date of Script (Reverse Chronological Order)	Script name	Script Description
March 27, 2001	**Soltip-ex.c**	**Script that exploits the Solaris tip Buffer Overflow vulnerability.**
March 26, 2001	Aspseek-exploit.pl	Remote buffer overflow exploit for the ASPSeek vulnerability.
March 26, 2001	Ddnsf.tar.gz	A powerful attack against DNS servers.
March 26, 2001	Manhole.c	A local exploit for the man vulnerability that bypasses non-executable stack patches.
March 26, 2001	Mdcrack-0.7.tar.gz	A brute forcer for MD5 hashes, which is capable of breaking up to 6 character passwords within hours, and 8 character passwords within two days.
March 26, 2001	Promiscan002.zip	Windows software that searches for machines that are in promiscuous mode on the local network.
March 19, 2001	**Squash-dgux-x86.c**	**Script which exploits the DG/UX lpsched Long Error Message Buffer Overflow vulnerability.**

Trends

Probes/Scans:

There has been an increase in the number of scans and attacks to port 515 looking for the LPRng User-Supplied Format String vulnerability, Wu-Ftpd Remote Format String Stack Overwrite Vulnerability, ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability, and the rpc.statd Remote Format String Vulnerability.

There has been an increase in the number of suspicious probes and scans designed to find vulnerable domain name servers on corporate networks.

Backdoor-G and NetBus Trojan scans have increased in number.

Other:

NIPC has issued an advisory concerning a potential security vulnerability that exists in PDG Software, Inc. Shopping Cart software (versions prior to 1.63) which is being actively exploited. For more information, please see NIPC ADVISORY 01-007, located at: http://www.nipc.gov/warnings/advisories/2001/01-007.htm.

Numerous reports have been received indicating that the snmpXdmid vulnerability is actively being exploited which could allow a malicious user to gain root access. For more information, please see CERT® Advisory CA-2001-05, located at: http://www.cert.org/advisories/CA-2001-05.html.

Worms are being released based on well-known exploits such as Bind, LPRng, rpc-statd, and wu-ftpd.

A new worm, Linux.Lion.Worm, appears to be spreading rapidly across the Internet. It scans the Internet looking for Linux computers with the BIND TSIG vulnerability. It infects the vulnerable machines, steals the password file (sending it to a China.com site), installs other hacking tools, and forces the newly infected machine to begin scanning the Internet looking for other victims. For more information, please see the Virus Section and NIPC ADVISORY 01-005, located at http://www.nipc.gov/warnings/advisories/2001/01-005.htm.

A new version of a Trojan horse program, SubSeven 2.2, that is popular with computer intruders has been publicly released on the Web. For more information, please see the Trojan Section.

On January 29 and 30, 2001, VeriSign, Inc. issued two certificates to an individual fraudulently claiming to be an employee of Microsoft Corporation. Any code signed by these certificates will appear to be legitimately signed by Microsoft when, in fact, it is not. For more information, please see NIPC ADVISORY 01-006, located at: http://www.nipc.gov/warnings/advisories/2001/01-006.htm, or CERT® Advisory CA-2001-04, located at: http://www.cert.org/advisories/CA-2001-04.html.

A software package has been released which, if used maliciously, may disable a victim's computer or network's IDS by flooding it with Internet traffic emanating from several random Internet Protocol (IP) addresses simultaneously. For more information, please see NIPC ASSESSMENT 01-004, located at: http://www.nipc.gov/warnings/assessments/2001/01-004.htm.

Viruses

NOTE: At times, viruses may contain names or content that may be considered offensive.

Adore (Alias: Red Worm) (Linux Worm): This worm has been reported in the wild and is similar to the Ramen and Lion worms. The worm is designed to create backdoors in the security of Linux systems and send information identifying the compromised systems to four different e-mail addresses that are hosted on servers in China and the United States. It scans the Internet and checks Linux hosts to determine whether they are vulnerable to any of the following well-known exploits: LPRng, rpc-statd, wu-ftpd and BIND (LPRng is installed by default on Red Hat 7.0 systems). The Adore worm replaces only one system binary (ps) with a Trojaned version and moves the original to /usr/bin/adore. It installs the files in /usr/lib/lib and sends an e-mail to the following addresses:

adore9000@21cn.com
adore9000@sina.com
adore9001@21cn.com
adore9001@sina.com

It attempts to send the following information:

/etc/ftpusers
ifconfig
ps -aux (using the original binary in /usr/bin/adore)
/root/.bash_history
/etc/hosts
/etc/shadow

The worm also runs a program called ICMP, which listens and sets the rootshell to accept connections on port 65535, acting as a backdoor, if the received packet length is equal to the one specified in the sourcefile. After infecting a machine and sending information about the computer through e-mail, the worm waits until 4:02 a.m. and then deletes all its files, except the backdoor.

BW-770-b (DOS Executable File Virus): This is a DOS executable file virus, which is dropped by the Troj/Futs Trojan horse (See Trojan Section). When the virus is executed it infects COM and EXE files in the current directory, increasing their length by 770 bytes. Occasionally the virus will do one of the following:

- Display the message: "Don't be a fool, fuck the school"
- Attempt to format the hard drive
- Cause the computer to beep constantly until it is rebooted

The virus was written with the Biological Warfare virus construction kit.

Butterfly.302 (DOS-based Memory Resident Virus): This is a DOS-based, memory-resident virus that only infects .com files.

HLLC.Laufwerk.7040 (Companion Virus): This virus is written in a high-level language. Using random file names, the virus makes multiple copies of itself that are 7040 bytes in size. This virus only replicates if you run one of these files, but does not infect or modify any files on your computer.

JS_WIRETAP.DEMO (Aliases: WIRETAP.DEMO, JS/WIRETAP.DEMO) (JavaScript Virus): This malware is only a demonstration of the e-mail wiretap security hole. Due to the existing vulnerabilities of some e-mail client software it is possible to execute embedded scripts. Other similar attacks are also possible on this security hole.

KC.1238 (DOS-based Virus): This is a DOS-based, memory-resident, stealth virus that only infects .com files that are run from a DOS window.

LittleChild.754 (DOS Virus): This virus is a non-memory-resident virus that infects only .com files when it is run from DOS.

PE_CIH.1122 (Aliases: CIH.1122, Win32/CIH, Win95.CIH, Win32CIH1.4, CIH.C) (File Infector Virus): This memory-resident virus infects all EXE PE and ZIP files. It inserts its virus code to empty spaces in every section of a target file so that the size of an infected file does not change. It also has a destructive payload that overwrites garbage to the infected hard disk so that it becomes un-bootable.

PE_HOOY.8192 (Aliases: W95.Hooy.8192.Dr, W95/Hooy.8192, HOOY.8192) (File Infector Virus): This non-destructive, memory-resident, parasitic Win32 virus appends its virus code at the last section of an infected file. Upon execution, this virus installs itself in memory so that it infects EXE files when they are executed. It appends its 8,192 bytes of virus code at the last section of the host file and changes the entry point of the file so that it points to itself. The virus also infects some executable files in the Windows and Windows System directories that have not been opened.

VBS/Anjulie@MM (Aliases: Angel (F-Secure), AnJulie.A (CA), VBS.Rewind.A@mm (NAV)) (Visual Basic Script Worm): This VBScript worm attempts to mail itself to all recipients in the Microsoft Outlook address book and drops the W95/CIH.1122 file infector virus. When run, the script copies itself to the WINDOWS TEMP directory as T4UMHF5.vbs and drops the file ALE32.EXE in the same directory. It creates a registry run key value to load the script at startup:

HKLM\Software\Microsoft\Windows\CurrentVersion\
RunServices\T4UMHF5=C:\WINDOWS\TEMP\T4UMHF5.VBS

VBS/Breberka.A@MM (Aliases: I-Worm.Breberka, BREBERKA.A, VBS/Gorum.gen@MM) (Visual Basic Script Worm): This Visual Basic Script worm propagates via e-mail in Microsoft Outlook. It also scans for fixed and remote drives or network drives connected to the infected computer and then drops copies of itself in the scanned drives as BREBERKA.TXT. VBE as well as a DROPPER.COM Trojan program.

VBS_LEE.A (Aliases: LEE.A, I-VBS LindaA@mm, VBS/pica.worm.gen, I-Worm.Lee, VBS/Linda-A) (Visual Basic Script Worm): This worm is capable of sending unsolicited e-mail to all entries listed in the Microsoft Outlook address book of the infected user. This virus can also send files via Internet Relay Chat (mIRC) and PIRCH.

VBS.Pleh.A@mm (Visual Basic Script Worm): This worm sends itself to e-mail addresses in the Microsoft Outlook address book. It overwrites files on local and remote drives, including files with the extensions .mp3, .pwd, .exe, .mp2, .doc, .avi, .mpeg, or .htm. The contents of these files are replaced with the source code of the worm, destroying the original contents.

VBS_VBSWG.GEN (Aliases: VBSWG.GEN, VBS/VBSWG.gen@MM): This is a worm that is generated by a Trojan, TROJ_VBSWG_2B (See Trojan Section). The features of this worm can be determined by the virus writer based on the options in worm generator console. It can replicate via the Microsoft Outlook application and sends itself as an attachment to all addresses listed in the infected user's address book. The subject and the message body of the e-mail vary. This worm can also be configured to replicate via Internet Relay Chat (mIRC) so that it can create a SCRIPT.INI file that allows it to send copies of itself via mIRC when the infected user joins a channel. This worm also infects VBS and VB Editor files contained in an infected system. When it is configured to infect files, it searches for and then infects VBS or VBE files upon execution. This worm arrives in many formats. It can be in an encrypted form that employs two different encryption routines, which lead to additional difficulty in its detection. It employs a mechanism that appends its code to an EXE file so that it arrives in EXE format as well. For its payload, it may be configured to display a message box, visit a particular URL, or shut down an infected system. The displayed message, the number of times its payload executes, and the trigger date for its payload depends on how it is configured.

VBS/VBSWG-V (Visual Basic Script Worm): This is an encrypted worm that uses Outlook mIRC and Pirch to spread. This worm arrives as an attachment named "Cindy12yr.vbs" in an e-mail with the subject line: "Check out this preteen pic!!." The body of the e-mail contains pornographic text. The worm will attempt to overwrite VBS and VBE files on network drives.

VBS.Yabran.A@mm (Visual Basic Script Worm): This is a simple worm, which spreads from an infected computer by e-mailing itself to everyone listed in the Microsoft Outlook address book.

W32.Check.Worm (Alias: W32.Adult) (Executable File Worm): This is a worm written in Visual Basic. Using the Windows Internet Relay Chat (IRC) chat client mIRC, it spreads to computers that have Windows 95/98/ME installed in the default location. If the worm is unable to find mIRC in the default installation path, it modifies the Autoexec.bat file so that when the computer is restarted, the Windows file Kernel32.dll is deleted. This IRC worm attempts to disguise itself as an Adult Checker. The "payload" is triggered when this Adult Checker window is closed.

W32/Lindose (Aliases: ELF/Lindose, W32/Winux, W32.PEElf.2132) (W32 Executable File Virus and Linux ELF Executable File): This is the first cross-platform virus to infect both Windows PE executable files and Linux ELF executable files. When the virus is executed, it searches for PE and ELF files in the current directory and other directories above the current one in the directory tree. If a PE file is found, the virus looks for the .reloc section, and if the section is large enough, overwrites it with the virus code. If an ELF executable file is found, the virus appends the uninfected original host code to the end of the file, so that it can be restored and run in memory after the virus code stops running. It also overwrites the original entry point with the virus code. The virus body contains the text:

"[Win32/Linux.Winux] multi-platform virus by Benny/29A"

and

"This GNU program is covered by GPL."

W97M/JulyKiller.D (Word 97 Macro Virus): This virus infects Microsoft Word 97 documents and the NORMAL.DOT global template. On 14 February, W97M/JulyKiller writes a certain text 50 times (in the active document).

W97M/Marker.EF (Word 97 Macro Virus): This virus infects Microsoft Word 97 documents and the NORMAL.DOT global template. The virus deletes all files with a .DOC or .DOT extension that it located in the Word start directory.

W97M.Mxc.A (Word 97 Macro Virus): This Macro Virus is a simple macro virus that will infect on opening an infected document. It will export its viral source code to "C:\tk.mxc." It will also disable the Security setting under Office 2000.

W97M.Odious.E (Word 97 Macro Virus): This is a simple macro virus that displays a message box and creates a text file. It displays the message:

Dont Panic This is an unDamage Virus - It was modified By Us To do no harm!!!

It also creates the C:\hate_h.vir text file, in which it inserts the text:

Your Office is infected with hate_h virus.

W97M.String.C (Word 97 Macro Virus): This virus is similar to many other Microsoft Word macro viruses. It does not alter any settings, and does not contain a malicious payload.

W97M.Thus.BQ (Word 97 Macro Virus): When you open a document, the virus first conceals itself by switching off the Macro Virus Protection option. The virus then infects the normal template (Normal.dot) and all open documents. When you create a new document or close a document, the virus executes the "document open" routine. The date is then checked, and if it is the 13th or 26th of the month, the payload is deployed and the virus attempts to shut down Windows.

WM97/Bablas-BQ (Word 97 Macro Virus): This is a Word macro virus. On Fridays, the virus will display a message box containing the following text:

"Kupersembahkan virus macro ini untuk seorang kawan berinisial Gemini 15/6/79. Semoga ia masih mengingatku. Terima kasih kepada teman-teman yang membantu tersebarnya virus ini. Jika Anda mendapati pesan ini, abaikan saja karena virus ini tidak berbahaya sama sekali.

TULUNGAGUNG KOTA BERSINAR
Sinar datang dari Surga."

WM97/Bottra-A (Word 97 Macro Virus): This is a Word macro virus that infects Microsoft Word documents and does little other than replicate. The virus creates a file called C:\tk.mxc (which is not viral) which is used during replication.

WM97/Marker-GW (Word 97 Macro Virus): There is a 1 in 3 chance that this virus will change the data in the File|Properties|Summary sheet of the infected file to include:

Title: Ethan Frome
Author: EW/LN/CB
Keywords: Ethan

WM97/Marker-GX (Word 97 Macro Virus): The virus keeps a log of user addresses and machine names, which is updated on each new infection. It may attempt to FTP this logfile information on Sundays.

WM97/Marker-GY (Word 97 Macro Virus): This is a Word macro virus. There is a 1 in 3 chance that this virus will change the file summary information to:

Title: Ethan Frome
Author: EW/LN/CB
Keywords: Ethan

WM97/Marker-MR (Word 97 Macro Virus): Whenever a document is closed there is a 1 in 3 chance of the data in the title field of the File|Properties|Summary sheet changing to Ethan Frome.

WM97/Wrench-L (Word 97 Macro Virus): This virus is a minor variant of the WM97/Wrench-G Word macro virus. The virus will display the office assistant if the user tries to open the VB Editor, change the document font, or print the document. The virus drops a file called ascii.vxd in the root directory, which is used as part of the replication process.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. NOTE: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor-JZ	N/A	CyberNotes-2001-02
BAT.Install.Trojan	N/A	CyberNotes-2001-04
BAT.Trojan.DeltreeY	**N/A**	**Current Issue**
BAT.Trojan.Tally	**N/A**	**Current Issue**
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01
BioNet	**3.13**	**Current Issue**
BSE Trojan	**N/A**	**Current Issue**
DLer20.PWSTEAL	N/A	CyberNotes-2001-05

Trojan	Version	CyberNotes Issue #
Flor	N/A	CyberNotes-2001-02
HardLock.618	N/A	CyberNotes-2001-04
JS.StartPage	**N/A**	**Current Issue**
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
Troj/Futs	**N/A**	**Current Issue**
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	**N/A**	**Current Issue**
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VBSWG_2B	**N/A**	**Current Issue**
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.PSW.M2.14	**N/A**	**Current Issue**
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05

Trojan	Version	CyberNotes Issue #
Trojan.Taliban	**N/A**	**Current Issue**
Trojan.W32.FireKill	**N/A**	**Current Issue**
Trojan/PokeVB5	**N/A**	**Current Issue**
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	**N/A**	**Current Issue**

BAT.Trojan.DeltreeY: This Trojan is a simple batch file that contains the command deltree /y C:*.*

BAT.Trojan.Tally: This Trojan horse attempts to move all the files from the Windows directory to C:\Win9x. It creates the file Tally.t, which uses the Windows debug function to convert Tally.t to Tally.ans. Tally.ans is the file that performs the malicious action.

BioNet: This is a remote access Trojan that has an edit server program. It also has a CGI notify, which allows BioNet to use CGI scripts to do almost anything. It has a schedule command feature that allows the BioNet server to activate any other feature at certain times, such as a specific day or hour, or even when the computer comes online. BioNet has a few stealth features, including the ability to use a random port each time the server is started. Another feature is the ability to delay the server from starting for x number of days or reboots.

BSE Trojan: This is an Assembly remote access Trojan that only has three features and does not infect. The server features are: restart or shutdown Windows; and System lockup.

JS.StartPage: This is a Trojan horse program, which alters the default home page of Microsoft Internet Explorer. It sometimes arrives as a file with the .hta extension. This file is an HTML application, and runs only if the Windows Scripting Host is installed. When JS.StartPage is executed, it makes changes to the following registry key:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page

TROJ_ASIT (Alias: ASIT): This is a hacker tool that floods the Windows folder of an infected system with texts containing explicit remarks. Upon execution, it allows a remote hacker access to an infected system. It also enables a remote hacker to drop text files named as follows in the Windows folder of an infected system:

FUCKxxxx.TXT
xxxx is any number from 1 to infinity

This Trojan has a console that contains the following data:

Title: C:\AwShit 1.0 (Windows Bomber)
Pre-Installed Bitch 1 <Clear button>
Pre-Installed Bitch 2 <Clear button>
Pre-Installed Bitch 3 <Clear button>
Pre-Installed Bitch 4 <Clear button>
Pre-Installed Bitch 5 <Clear button>
<Send 1> <Send a Couple> <Send Many>

Troj/Futs: This Trojan has been reported in the wild and is designed to integrate with Novell NetWare. When executed, the Trojan horse presents the user with a screen containing various options. These include filling the local hard disk, erasing the CMOS memory, deleting all files on the local hard disk, causing the NetWare server to beep constantly, making various NetWare queries or activating a multi-user chat system. The Trojan horse includes a "boss screen" option, which pops up a fake Borland Pascal 7.0 window. Troj/Futs also has an option to drop the BW-770-b DOS executable file virus.

Trojan/PokeVB5: This is a Trojan whose aim is to allow access to other systems. The Trojan goes memory resident and the payload consists of restarting Windows and asking for the user's access password.

Trojan.PSW.M2.14: This Trojan is a password-stealing program, which releases confidential information. Upon execution, Trojan.PSW.M2.14 creates a copy of itself as \Windows\System\Rundll16.exe. It then adds the subkey, \Rundll16 system module, to the registry key:

HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Run

The subkey contains the following value data: Rundll16.exe. Trojan.PSW.M2.14 then sends to the author an e-mail message that contains the stolen passwords.

Trojan.Taliban: This Trojan often appears in your e-mail as an attached .exe file. This .exe file, which has no standard name, disguises itself as a IQ test. Once activated, it presents you with a ten-question IQ test. Question numbers one, three, and six are "key questions." Answering question three correctly, or answering questions one or six incorrectly, will active the payload, which then attempts to destroy all critical files in the C:\Windows folder. Regardless of the status of the "key questions," if a perfect score is obtained, no damage is done. If the program terminates without causing any damage, a request is displayed on the monitor asking you to mail out this program to all your friends.

TROJ_VBSWG_2B (Aliases: VBS Worms Generator 2 beta, VBSWG_2B): This is another version of the Visual Basic Script (VBS) Worms Generator. It is the beta of the 2nd version and is capable of creating VBS worms that can propagate via MS Outlook and/or Internet Relay Chat (mIRC). It can also generate different variants that have unique characteristics.

Trojan.W32.FireKill (Alias: Trojan.Win32.FireKill): This is a Trojan horse that can disable the Norton AntiVirus software if the current virus definitions are not installed. When executed on a computer on which Norton AntiVirus is installed but with outdated virus definitions, Trojan.W32.FireKill will disable Auto-Protect. When you then try to scan using Norton AntiVirus, the system stops responding and the display may go blank. It is also capable of disabling other AntiVirus products.

W32.BrainProtect: This is a mIRC script-dropping Trojan horse. When executed, it creates a copy of itself as C:\Pinkycerebro.scr. It then creates the file \Mirc\Mirc.hst and modifies Mirc.ini by appending the following string to the end of the file: n=mirc.hst. This will force Mirc.exe to execute the contents of the Mirc.hst script file.